UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,660	05/01/2006	**Richard Middleton Hicks**	9664-0003	8461

73552 7590 10/26/2011

Stolowitz Ford Cowger LLP
621 SW Morrison St
Suite 600
Portland, OR 97205

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	**PAPER NUMBER**
2437	

MAIL DATE	DELIVERY MODE
10/26/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,660	HICKS, RICHARD MIDDLETON	
	Examiner	Art Unit	
	PAUL CALLAHAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,2,4-6,8-12,14-20,22,24-28,30-34,36,37 and 39* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,2,4-6,8-12,14-20,22,24-28,30-34,36,37 and 39* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is prompted by the Applicant's response filed 8-10-2011.

2. Claims 1, 2, 4-6, 8-12, 14-20, 22, 24-28, 30-34, 36, 37 and 39 are pending and have been examined.

Response to Arguments

3. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection necessitated by the latest amendment.

The Applicant argues that the Cowie, Feigen and Richie references fail to teach the newly added features of *"...identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files..."*, and *"...displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program..."* However, the Examiner has applied new art: Vella, US 2003/0212913 A1 to teach these new limitations.

The Applicant argues that the combination of Cowie and Feigen is improper since the Feigen reference is such that it teaches away from the combination. The Applicant asserts that there is a fundamental difference in functionality of the system of Cowie and Feigen that would require undue modification. However, the Examiner Maintains that the Feigen reference was used only to teach the concept of examining

short segments of the executable code of a program for a signature by comparison with known signatures. The system of Cowie is compatible with this since both are using a process of comparison of s signature of a suspect portion of code to known malware signatures.

***The Applicant is requested in the next response to identify where support is found in the Specification for the latest amendments to the claims. (See MPEP Sec. 714.02).**

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 2, 4, 5, 6, 8-10, 22, 24-28, 30-33, 37, and 39 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As for claim 1, this claim has been amended in the latest response to recite the new limitations: *"...identifying, with a processing device, computer files comprising*

software code, wherein the steganographic program is excluded from the identified computer files…", and "*…displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program…*". The Applicant's Specification does not describe these steps where the steganographic program is excluded, or the display of a list, developed based on a comparing step of programs modified by the steganographic program.

As for claims 2, 4, 5, 6, 8-10, 33 and 39, these claims are dependent on claim 1 and do not cure its deficiency. Therefore hey are rejected on the same basis as that claim.

As for claim 31, this claim has been amended in the latest response to recite the new limitations: *"…identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files…"*, and "*…displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program…*". The Applicant's Specification does not describe these steps where the steganographic program is excluded, or the display of a list, developed based on a comparing step of programs modified by the steganographic program.

As for claims 22, 24, 25, 26-28, 30, 32 and 37, these claims are dependent on claim 1 and do not cure its deficiency. Therefore hey are rejected on the same basis as that claim.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1, 2, 4, 5, 6, 8-10, 22, 24-28, 30-33, 37, and 39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As for claims 1 and 31, these claims have been amended in the latest response to recite the new limitation in bold:

"...locating a steganographic program comprising executable code that includes software calls that introduce steganographic items into a computer file;

obtaining a steganographic signature by reading a partial section of the executable code;

identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files;

obtaining one or more test signatures by reading partial sections of the software code;

It is not clear from the context of the claim, which section of code is referred to in the last listed limitation above. As presented, It could apply to the steganographic

program code, or the computer files from which the steganographic program is excluded.

Claims 2, 4, 5, 6, 8-10, 22, 24-28, 30, 32-33, 37, and 39 are dependent on claims 1 and 31 and do not cure the deficiencies of those claims. Therefore the dependent claims are rejected on the same basis as are claims 1 and 31.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 2, 5, 6, 8-12, 14-16, 18-20, 22, 24-26, 28, 30-34, 36, 37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cowie et al. US 2003/0023865 A1, Feigen et al., US 2002/0138554, Vella, US 2003/0212913 A1.

As for claims 1 and 39, Cowie teaches a method, comprising, obtaining a signature by reading code comprising a partial section of a program, (fig. 5: element 18, [0015], [0034], [0048]), comparing the signature with one or more computer files (fig. 5: element 18, [0015], [0034], [0048]), and, displaying based on said comparing, a listing of which of the one or more computer-files provide a match with the signature (fig. 6 element 46, [0050]). Cowie does not teach that the code read is executable code or that

partial sections of the software code are read. However Feigen does teach these features ([0009], [0010]: a hash signature of a block of code where the block is a portion of a larger executable [0014]) Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would increase the probability of detecting hidden malware code in a file. Cowie fails to explicitly teach the feature where the computer-program is a steganographic program that includes software calls, and the steps of identifying with a processor files comprising software code wherein the steganographic program is excluded form the identified computer files, and a step of displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program. However Vella does teach such a feature ([0060]:program calls, fig. 3, [0064] a list of programs called by the steganographic executable is displayed). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would extend the types of programs that can be evaluated for embedded malware detectable via the comparison step of Cowie.

As for claim 2, Cowie teaches a method according to claim 1 wherein the indication incorporates an identification of the item's location in the computer system ([0048]-[0050]).

As for claim 5, Cowie teaches a method according to claim 1, where an asserted file type is ignored when comparing files with the signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 6, Cowie teaches a method according to claim 1 wherein the step of comparing the signature with files is for each file preceded by checking the respective real file type by reading the start of the file and excluding computer files having prearranged initial byte sequences from comparing with the signature (fig. 6 element 32, [0049]: initial byte sequence is used to determine if file is a WIN32 PE file and if not, exclude it from further processing).

As for claims 8, 18, and 28, each of these claims is directed to the case where the file is a deleted or logical wastebasket file. Cowie teaches this feature ([0030]: WIN32 PE file type includes such files).

As for claim 9, Cowie teaches a method according to claim 1 wherein the one or more computer files comprise self-extracting executable files ([0006]).

As for claim 10, Cowie teaches a method according to claim 1 wherein some prearranged files are not identified in the listing despite containing software code which matches a signature ([0050]).

As for claims 11, the claim is directed towards the apparatus carrying out the method of claims 1. Claim 11 recites substantially the same limitations as claims 1 and therefore is rejected on the same basis as that claim.

As for claim 12, Cowie teaches a method according to claim 1 wherein the indication incorporates an identification of the matching signature ([0048]-[0050]).

As for claim 14, Cowie teaches the apparatus according to claim 11 where the code of the signature comprises a continuous sequence of the partial section of the program code (fig. 5: element 18, [0015], [0034], [0048]).

Claim 15 represents the apparatus carrying out the method steps of claim 5. Claim 15 recites substantially the same limitation as claim 5 and is therefore rejected on the same basis as that claim.

As for claim 16, Cowie teaches the apparatus of claim 11 wherein the partial section of code comprises a start of the computer file, and wherein computer files having a prearranges initial byte sequence are excluded for comparison (fig. 6 element 32, [0030]: file header is examined to determine if the file is a WIN32 PE file, a byte sequence is inherent for any such sequence of digital data).

As for claim 19, Cowie teaches the apparatus according to claim 11 wherein the one or more files comprise polymorphic files (fig. 5 element 16, [0048]: Trojan containing files include polymorphic malware).

As for claim 20, Cowie teaches the apparatus according to claim 11 wherein one or more predetermined files are not indicated despite containing code which matches a signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 22, Cowie teaches the computer-program product of claim 11 further comprising identifying a steganographic item responsible for the match ([0048] - [0050]: Trojan signature).

As for claim 24, Cowie teaches the computer-program product of claim 11, wherein the signature comprises a continuous sequence of program code but not more than 5% or less than 0.167% of the program (fig. 5: element 18, [0015], [0034], [0048]: header data is used for the signature).

As for claim 25, Cowie teaches the computer-program product of claim 31 wherein an asserted file type is not compared with the signature ([0048], [0050]: non WIN32 PE files excluded).

As for claim 26, this claim is directed towards the computer-program product that

directs a processor to carry out the method of claim 16. Claim 26 recites substantially the same limitations as claim 16 and is therefore rejected on the same basis as that claim.

As for claim 30, this claim is directed towards the computer-program product that directs a processor to carry out the method of claim10. Claim 30 recites substantially the same limitations as claim 10 and is therefore rejected on the same basis as that claim.

As for claim 31, the claim is directed towards a computer program product that directs a processor to carry out the method of claim 1. Claim 31 recites substantially the same limitations as claims 1 and is therefore is rejected on the same basis as that claim.

As for claim 32, Cowie teaches the computer-readable medium of claim 31, wherein the method further comprises executing the one or more files, and wherein the comparison is made prior to executing the one or more files ([0030]-[0031]: identification of banned game programs prior to being run on a business computer).

As for claim 33, Cowie teaches the method of claim 1, further comprising running a virus checking program while comparing the signature with one or more computer files (fig. 5: element 18, [0015], [0034], [0048]: the signature comparison algorithm of

Cowie is an anti-viral program).

As for claim 34, Cowie teaches the apparatus according to claim 15, wherein the one or more predetermined file types are a graphics editor ([0030]: WIN32 PE file type includes graphics editors).

As for claim 36, Cowie teaches the computer apparatus according to claim 11, wherein the apparatus is further configured to analyze the one or more test signatures with a virus checking program in combination with the comparison with the steganographic signature (fig. 5, fig. 6, [0049], [0049]).

As for claim 37, the claim is directed towards the computer readable medium that directs a processor to carry out the method of claim 11. Claim 37 recites substantially the same limitations as claim 11 and is rejected on the same basis as that claim.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cowie, Atkinson and Richer as applied to claim 1 above, and further in view of Charbonneau, US 7,526,654.

As for claim 4, the combination of Cowie, Atkinson and Vella teaches the method according to claim 1, but not explicitly wherein the code that is read is a .DDL file. However, Charbonneau does teach such a feature (col. 5 lines 10-20). Therefore it

would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie and Richer. It would have been obvious to do so since this would extend the types of files where embedded malware is detectable via the comparison step of Cowie.

Allowable Subject Matter

11. Claims 17 and 27 are not rejected over prior art, but instead are rejected only under 35 USC Sec. 112. These claims would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, and if the rejections under 35 USC Sec. 112 were overcome.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Eleni Shiferaw, can be reached on (571) 272-3867. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/PEC/
AU2437

/Michael Pyzocha/
Primary Examiner, Art Unit 2437